



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/505,951	02/15/2000	Simon Robert Walmsley	AUTH08US	5608
<div>Kia Silverbrook Silverbrook Research Pty Ltd 393 Darling Street Balmain, 2041 AUSTRALIA</div>				
<div>7590 01/03/2008</div>			<div>EXAMINER DAVIS, ZACHARY A</div>	
			<div>ART UNIT 2137</div>	<div>PAPER NUMBER</div>
			<div>MAIL DATE 01/03/2008</div>	<div>DELIVERY MODE PAPER</div>

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/505,951

Applicant(s)

WALMSLEY ET AL.

Examiner

Zachary A. Davis

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 October 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4,5,7-14 and 16-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4,5,7-14 and 16-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 29 October 2007 has been entered.
2. By the above submission, Claim 1 has been amended. No claims have been added or canceled. Claims 1, 2, 4, 5, 7-14, and 16-20 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 2, 4, 5, 7-14, and 16-20 have been considered but are moot in view of the new ground(s) of rejection.

The Examiner notes that Applicant's arguments make mention of a hash value (see pages 6-7 of the present response); however, nowhere in the claims is there recited a hash value.

Examiner's Note

4. First, the Examiner notes that it appears that the amendments to the claims (specifically, the added and deleted text) appear to have been printed in a different color (presumably red) or at least a shade of grey. However, because the documents are scanned into the system in black and white, this differently colored text is difficult to read in places. It is strongly recommended that all text be shown only using black ink in all future submissions.

5. In response to the Examiner's note in the previous Office action (mailed 13 September 2007), Applicant has stated that the amendments to independent Claim 1 clarify "that the 'trusted' chip is considered to be trusted so long as each call of the test function using the first number returns a mismatch" as described in the present specification (see page 6 of the present response). However, the Examiner again notes that this appears to contradict the generally accepted definition of the term "trusted". If there is any concern that the ChipT (as described in the specification at page 66, line 17-page 67, line 3 and elsewhere, corresponding to the claimed "trusted chip") may be replaced and may need to be authenticated as described in at least the noted portions of the specification, and if the trusted chip may at some point not be considered to be trusted as stated by Applicant in the present response, then it would appear that the chip is not, in fact, totally trusted in the traditional sense of the word. That is, if a test

Art Unit: 2137

may reveal that a chip is not trusted, then it is not clear how the chip would be considered to be trusted in general.

Claim Rejections - 35 USC § 112

6. The rejection of Claims 1, 2, 4, 5, 7-14, and 16-20 under 35 U.S.C. 112, second paragraph, as indefinite, is NOT withdrawn. Although the amendments to the claims have addressed the issues of indefiniteness raised in the previous Office action, they have also introduced new issues of indefiniteness as set forth below.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 2, 4, 5, 7-14, and 16-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "encrypting the random number by the symmetric encryption function using the second key, in the trusted chip, to produce a second random number" in lines 25-26 of the claim. It is not clear whether the limitation "the random number" is intended to refer to the "random number" mentioned earlier in the claim (see, for example, the generation of the secret random number at lines 5-8 of the claim) or to the "plural and random number of times" recited in line 23. This renders the claim indefinite.

Claims not explicitly referred to above are rejected due to their dependence on and/or incorporation of all the limitations of rejected Claim 1.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1, 2, 4, 7-14, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carmon et al, WIPO Publication WO99/10180, in view of Sony Corporation (Kusakabe), European Patent EP 0817420, Spies et al, US Patent 5689565, Goto, US Patent 5617429, and Sibert, US Patent 7243236.

In reference to Claim 1, Carmon discloses a validation protocol for determining authenticity of a printer consumable (page 4, line 20-page 5, line 10) including the steps of providing a printer containing a trusted authentication chip and a printer consumable containing an untrusted authentication chip (page 11, line 20-page 12, line 2); generating and encrypting a random number in the trusted authentication chip (page 12, lines 8-12); encrypting the random number in the untrusted authentication chip (page 12, lines 9-11); and comparing the two encrypted random numbers, where if the two encrypted numbers match, then the untrusted chip is considered to be valid and use of the consumable is authorized, or else the untrusted chip is considered to be invalid and

Art Unit: 2137

use of the consumable is denied (page 12, lines 13-15; see also page 11, lines 10-12).

However, Carmon does not explicitly disclose encryption with two different keys.

Sony discloses an authentication method (see Figures 7- 9, Claim 1, and column 2, line 49-column 3, line 17) in which a random number is generated by a random function (column 8, lines 12-17) and encrypted with a symmetric encryption function using a first key in a first apparatus (column 9, lines 13-17). The encrypted random number is sent to a second apparatus (column 9, lines 18-21) and decrypted with a symmetric decryption function using the first key (column 9, lines 31-37), and then encrypted with the symmetric encryption function using a second key (column 9, lines 41-48) and sent to the first apparatus (column 9, line 57-column 10, line 2). The encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28). The two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). Therefore, it would have been obvious to modify the protocol of Carmon to use the specifics of the method taught by Sony, in order to authenticate an untrusted device as an authorized party for communication (see Sony, column 10, lines 31-35; column 14, lines 12-15; see also column 1, line 57-column 2, line 48).

Further, neither Carmon nor Sony discloses the calculation and comparison of a digital signature as a step of the authentication method. Spies discloses a cryptographic system and method that includes generating a digital signature of a

Art Unit: 2137

document (column 12, lines 6-13) and encrypting the document and digital signature under the same symmetric encryption key in a sending device (column 12, lines 14-27, noting especially the equation at line 25). Spies further discloses decrypting the document and signature at a receiving device (column 13, lines 15-22) and verifying the signature (column 13, lines 20-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Sony by including the steps of generating a digital signature of the random number (the "document") and encrypting the signature with the random number in the first apparatus, and of decrypting and verifying the signature in the second apparatus, in order to authenticate the sending of the random number (see Spies, column 13, lines 26-32) and more generally to allow for greater security, privacy, authenticity, and integrity in the system (see Spies, column 2, lines 1-4).

Additionally, although Carmon, Sony, and Spies disclose encrypting the random number in the trusted chip and comparing the encrypted number with the second number (as above, at least Sony, column 9, lines 41-48, column 9, line 57-column 10, line 2, and column 10, lines 21-39), none of Sony, Carmon, and Spies explicitly discloses calling a function using a first number such that a comparison never returns a match. Goto discloses a method in which a wrong expected value is passed to a function in order to force the function to output an error result (see column 16, lines 21-58, especially lines 42-58). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Carmon, Sony, and Spies by including the option of sending an intentionally wrong value in order

Art Unit: 2137

to increase reliability by verifying that the system can properly detect an error (see Goto, column 16, lines 14-20).

Still further, although Carmon, Sony, Spies and Goto disclose passing an incorrect expected value to a function in order to force the function to output an error result (as above, Goto, column 16, lines 21-58) and encrypting the random number in the trusted chip and comparing the encrypted number with the second number (as above, at least Sony, column 9, lines 41-48, column 9, line 57-column 10, line 2, and column 10, lines 21-39), none of Carmon, Sony, Spies, and Goto explicitly discloses making a plural and random number of comparisons with the intentionally incorrect value before comparing the encrypted number with the second number. Sibert discloses a method in which testing steps are repeated a random number of times in order to provide a reasonable probability that the application responding to the tests has not been modified (column 25, lines 13-40, especially lines 30-35; see also Figure 22A). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Carmon, Sony, Spies, and Goto to include performing the tests with the intentionally incorrect values a random number of times in order to provide a reasonable probability that the application has not been modified (Sibert, column 25, lines 30-35) and to help protect against inauthentic modules (see Sibert, column 4, lines 17-57).

In reference to Claim 2, Carmon as modified above further discloses that the first and second keys are held in both the first and second apparatuses (i.e. trusted and untrusted chips, see Sony, Figure 9).

In reference to Claim 4, Carmon as modified above further discloses that the second apparatus (i.e. untrusted chip) holds a decryption function (see Sony, column 9, lines 31-37).

In reference to Claim 7, Carmon as modified above further discloses that the second apparatus monitors the time elapsed between steps of its processing (see Sony, column 10, lines 53-56).

In reference to Claim 8, Carmon as modified above further discloses that the test function generating the random numbers is held in the first apparatus (see Sony, column 8, lines 12-15). Additionally, Carmon as modified above discloses that if the second apparatus is not authenticated, the authentication process is terminated (Sony, column 10, lines 36-39).

In reference to Claim 9, Carmon as modified above further discloses that the first apparatus monitors the time elapsed between steps of its processing (see Sony, column 10, lines 6-7).

In reference to Claim 10, Carmon as modified above further discloses that it is determined if the second apparatus is valid (Carmon, page 12, lines 13-15; see also Sony, column 10, lines 31-35) or not (Carmon, page 12, lines 13-15, and page 11, lines 10-12; Sony, column 10, lines 36-39).

Claims 11-14 and 16-20 are system claims reciting limitations corresponding substantially to those of the methods of Claims 1, 2, 4, 5, and 7-10, and are thus rejected by a similar rationale.

11. Claims 5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carmon in view of Sony, Spies, Goto, and Sibert as applied to claims 1 and 11 above, and further in view of Schneier, *Applied Cryptography*.

Carmon as modified above discloses everything as applied to Claims 1 and 11 above. However, neither Carmon, Sony, nor Goto discloses the use of digital signatures, and Spies and Sibert do not explicitly disclose the use of digital signatures of 160 bits. Schneier discloses that hash functions can be used in the creation of digital signatures, and specifically discloses the use of 160 bit hashes (page 38, last paragraph). Therefore, it would have been obvious to modify further the previously modified method of Carmon to include digital signatures 160 bits in length in order to increase the speed of the signature algorithm (see Schneier, page 38, last paragraph-page 39, first full paragraph).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Kung, US Patent 5442342, discloses a system in which an authentication protocol is repeated at random times and in which challenge and response steps are conducted a random number of times.

Art Unit: 2137

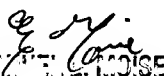
- b. Eckes et al, US Patent 6243832, discloses a testing system and method that performs various tests a random number of times.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


zad


EMMANUEL MOISE
SUPERVISOR